GAO

Report to the Chairman,
Committee on Science, House of
Representatives

December 1999

COMPUTER SECURITY

FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software

20000107 058

GAO
Accountability ★ Integrity ★ Reliability

GAO/AIMD-00-55

Printed copies of this document will be available shortly.

□ U.S. GOVERNMENT PRINTING OFFICE 1991-523-762

GAO Form 171 Rev. (3/99)

GAO

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-284308

December 23, 1999

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on Science
House of Representatives

To address the Year 2000 (Y2K) computing problem, public and private organizations across the nation have required large numbers of skilled computer programmers and systems managers to remediate, test, and review mission-critical systems. The nationwide demand for skilled programmers has raised questions as to whether key organizations used foreign nationals in their Y2K activities and how any such use was controlled. At your request, we identified the extent to which foreign nationals were involved in Y2K code remediation and subsequent code review activities at the Federal Aviation Administration (FAA)[1] and the agency's policies covering this involvement. On December 16, 1999, we briefed your office on the results of our work. The briefing slides are included in appendix I.

This report provides a high-level summary of the information presented at that briefing, including FAA's internal policies on using foreign nationals and its actual use of foreign nationals to remediate code and perform Y2K code reviews.

Results in Brief

FAA policy requires system owners and users to prepare risk assessments for all contractor tasks, and to have background investigations conducted for all contractor employees in high-risk positions. FAA also requires more limited background checks for moderate- and low-risk positions.

FAA's mission-critical systems requiring Y2K repairs—including some of the most important systems supporting the air traffic control system—were remediated by a mix of FAA and contractor employees and, in the case of commercial-off-the-shelf products, by the product vendors. While FAA did not maintain detailed information on individuals assigned to perform Y2K code remediation, FAA compiled some of this information in response to our request. In doing so, FAA identified instances where foreign nationals, employed by contractors, performed Y2K code remediation activities (i.e., code repair and/or testing). Of 153 mission-critical systems that were remediated, 15 had foreign national involvement--

---

[1] Code remediation involved repairing and/or testing systems software, while code reviews involved an independent, line-by-line review of a copy of the systems source code in order to identify any date dependencies.

including Chinese, Ukrainian, and Pakistani nationals. FAA was unable to provide any information about the individuals who performed code remediation for 4 of the 153 systems.[2]

With regard to code reviews, 20 key mission-critical systems have been, or are in the process of being, reviewed by two contractors who have foreign national employees. One code review contractor employed 36 mainland Chinese nationals while the other employed one Canadian national.

FAA, however, did not perform background searches—investigations or checks—on all of its contractor employees, as required by its policy. Specifically, the agency did not perform risk assessments and was unaware of whether it or the contractor had performed background searches on all of the contractor employees, including the foreign nationals. During our review, we found instances where background searches of foreign nationals were not performed. For example, no background searches were performed on the 36 mainland Chinese nationals who performed code reviews, according to FAA and the contractor, Primeon. FAA's failure to perform risk assessments, its lack of complete information on whether background searches were performed, and the fact that some foreign nationals did not undergo background searches have increased the risk that inappropriate individuals may have gained access to FAA's facilities, information, or resources. As a result, the air traffic control system may be more susceptible to intrusion and malicious attacks.

To address these issues, we are making recommendations to the FAA Administrator to improve FAA's security controls, identify the risk of malicious attacks on critical systems, and mitigate this risk. FAA has agreed with our recommendations in these areas and is moving to implement them. In addition, FAA officials stated that the agency has five layers of system protection, which they believe make the risk of intrusion extremely low. We anticipate evaluating the five layers of system protection as part of our continuing efforts to monitor the agency's progress in addressing computer security weaknesses.

Background

The Y2K computing challenge provides a vivid example of the need to protect critical systems. It illustrates the government's widespread dependence on systems and their vulnerability to disruption. During the Y2K conversion period, it was important that agencies be especially attuned to security issues because most agencies were under severe time constraints to make an unprecedented number of software changes. To the extent that this was not done, there is the danger of already weak controls being further compromised if agencies bypassed or truncated security in an effort to speed the software modification process. This increases the risk that erroneous or malicious code could be implemented and that inadequately tested systems could be rushed into use.

FAA's primary mission is to ensure safe, orderly, and efficient air travel throughout the United States. FAA's ability to fulfill this mission depends on the adequacy and reliability of the nation's air traffic control (ATC) system, a vast network of computer hardware, software,

---

[2]FAA officials stated that these four systems were commercial-off-the-shelf products.

and communications equipment that provides information to air traffic controllers and aircraft flight crews to ensure safe and expeditious movement of aircraft. FAA's ATC network is an enormous, complex collection of interrelated systems, including navigation, surveillance, weather, and automated information processing and display systems that reside at, or are associated with, hundreds of ATC facilities. Complex communications networks that separately transmit both voice and digital data interconnect these systems and facilities. As stated in our 1997 and 1999 reports on high-risk issues,[3] while the use of interconnected systems promises significant benefits in improved government operations, it also increases vulnerability to anonymous intruders who may manipulate data to commit fraud, obtain sensitive information, or severely disrupt operations.

In May 1998, we reported that FAA had weak computer security practices that jeopardized flight safety and concluded that FAA was ineffective in all critical areas reviewed—facilities physical security, operational systems information security, future systems modernization security, and management structure and policy implementation.[4] First, we reported that there were known weaknesses at many ATC facilities and that FAA was unaware of weaknesses that might have existed at other locations. Second, FAA was ineffective in managing systems security for its operational systems and was in violation of its own policy. Third, FAA was also not effectively managing systems security for future ATC modernization systems. Finally, we reported that FAA's management structure and implementation of policy for ATC computer security was ineffective, with security responsibilities distributed among three organizations that had all been remiss in their ATC security duties.

To address these weaknesses, we made a series of recommendations on physical security at FAA facilities, operational ATC systems security, future ATC modernization systems security, and management structure and policy implementation. FAA generally agreed with these recommendations and is in the process of implementing them. For example, in February 1999, FAA established a Chief Information Officer position with responsibility for developing, implementing, and enforcing the agency's information security policy. FAA's efforts to address physical and systems security weaknesses are underway.

FAA Security Policies Require Background Searches for Contractor Employees

Security program management and the related security controls over access to data, systems, and software programs are central factors affecting an organization's ability to protect its information resources and the program operations that these resources support. Federal agencies must protect the integrity, confidentiality, and availability of the information resources they rely on. FAA has a personnel security program order, a human resource policy manual, and a required contract clause that detail the requirements to be met by both

---

[3]High-Risk Series: Information Management and Technology (GAO/HR-97-09, February 1997) and High-Risk Series: An Update (GAO/HR-99-1, January 1999).
[4]Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD-98-155, May 18, 1998).

FAA and contractor employees and the actions FAA must take to ensure the credibility of these individuals. All three policies allow for the hiring of foreign nationals.

FAA's personnel security program order requires background investigations to be conducted for all FAA employees. In addition, this order requires system owners and users to prepare a risk assessment to determine the level of risk associated with contracts. Depending on the level of risk identified, the order then requires FAA to perform background searches—investigations or checks—for contractor employees who have comparable exposure to FAA's facilities, information, or resources.[5] Specifically, FAA requires that background investigations be conducted for contractor employees in high-risk positions and that more limited background checks be conducted for contractor employees in moderate- and low-risk positions.

FAA's human resource policy manual restricts hiring to U.S. citizens and nationals (residents of American Samoa and Guam) but allows for exceptions. Specifically, FAA may hire foreign nationals if (1) there are an insufficient number of well-qualified applicants and/or (2) there is an emergency, in which case, these individuals can be hired for a brief period of time. FAA officials noted that they were not aware of any instances in which FAA had hired foreign nationals.

In addition, FAA specifies that all of its contracts include a clause requiring contractors to hire U.S. citizens or aliens that are in the country legally as evidenced by either a "green card"[6] or the appropriate work visa, if work is likely to be performed at an FAA location. There was, however, some confusion about this clause within FAA. Some FAA employees considered the clause mandatory, while others considered it optional. As a result, the clause may have been inappropriately excluded from some of the contracts under which the Y2K code remediation activities were performed.

FAA Contractors Used Foreign Nationals for Y2K Code Remediation, But Not All Had Required Background Searches

FAA contractors used foreign nationals to help remediate mission-critical systems. Of 153 mission-critical systems that underwent code repair and/or testing, FAA advised us that 15 had some degree of foreign national involvement. These 15 systems included key ATC, communications, and administrative systems. For example, the Traffic Flow Management Infrastructure-Enhanced Traffic Management System, which is used to manage traffic flow across the National Airspace System, was remediated with the assistance of two Chinese, one Ethiopian, one Irish, and one Ukrainian. The Oceanic Automation System, which provides oceanic controllers with a situation display of aircraft positions, was remediated with the

---

[5]FAA does not require background searches on temporary contractor employees in low-risk positions.
[6]A "green card" is an alien registration receipt card, which documents that a foreign national has obtained permanent residency in the United States.

assistance of two British nationals. For four mission-critical systems, the degree of foreign national involvement, if any, was unknown by FAA.[7]

In overseeing these contracts, however, FAA did not adhere to its own policy requiring background searches to be performed for all contractor employees. When asked about the required background searches, the Y2K Program Office acknowledged that it was unaware of this requirement and did not know whether background searches had been performed for all contractor employees, including the foreign nationals involved in Y2K code remediation activities. The Associate Administrator for Research and Acquisitions stated the Office of Acquisitions was also unaware of the requirement to conduct background searches of contractor employees. In addition, we contacted three contracting officer technical representatives for key air traffic control systems, who stated that they had not performed background searches of contractor employees and, in some instances, did not review resumes.

By not following sound security practices, FAA has increased the risk of inappropriate individuals gaining access to FAA's facilities, information, or resources. As a result, there is inherently more risk that unauthorized changes, which are difficult to detect, could have been made during code renovation. In addition, program errors detected during testing may not have been identified for correction by individuals intending harm, resulting in potential system errors. While the scope of our work did not include identifying instances of code tampering or illegal activities and we did not find any such instances during our review, FAA's failure to adhere to its own policies has increased the risk that malicious code tampering may have occurred and may not have been detected.

FAA Contractors Used Foreign Nationals to Perform Y2K Code Reviews, But Not All Had Required Background Searches

FAA hired two contractors (Primeon and Computer Generated Solutions, Inc.) through the General Services Administration to perform Y2K code reviews of 20 mission-critical systems. With respect to Y2K compliance, code reviews entail a line-by-line analysis of a copy of the program source code to identify and evaluate date-related fields. According to FAA officials, a copy of the program source code was provided in its entirety to the contractors on various media (e.g., floppy disk, zip drive) and, in most cases, via express mail.[8] For each system, the contractors were required to provide a final report of the review results to the appropriate Y2K program office, and the system owners were expected to address any identified issues. FAA also required both contractors to sign nondisclosure agreements requiring the return or destruction of all copies of the program source code provided by FAA.

---

[7]FAA stated that these four systems--the BandWidth Manager Network, the Operation Support Telephone System, the ASU-400 Local Area Network, and CCMail--were commercial-off-the-shelf products.

[8]Code reviewers were not given direct access to operational systems, so they did not have the ability to directly insert code.

These code reviews have been and continue to be performed for systems that FAA has identified as the most important. To date, 17 of 20 systems have been reviewed with 2 currently being reviewed and 1 scheduled for review, according to FAA officials. The universe of systems is comprised of key ATC, communications, and administrative systems. For example, systems that have undergone code reviews include the Display System Replacement (DSR), which displays radar data to controllers in the en route environment, and the Automated Radar Terminal System IIIA (ARTS IIIA), which is the critical data processing system used in terminal radar approach control facilities to provide essential aircraft position and flight plan information to controllers.

Primeon was tasked with reviewing the code of eight mission-critical systems, including DSR, ARTS IIIA, and the Voice Switching and Control System (VSCS)—a critical system that supports ground-to-ground and air-to-ground communications in the terminal radar approach control environment. According to Primeon and FAA, 36 mainland Chinese nationals performed these code reviews. However, neither FAA nor Primeon had performed background searches on these employees.

Computer Generated Solutions, Inc. (CGS) was tasked with reviewing the code of 13 mission-critical systems,[9] including the Terminal Doppler Weather Radar and the Host Environment—the key information processing system in FAA's en route environment. According to CGS and FAA, there was one Canadian national whose involvement was limited to contract administration. This person should have undergone a criminal background investigation under CGS' recruiting policy, but FAA did not confirm that this had occurred. According to an FAA official, the agency did not conduct background searches of CGS' employees.

As stated earlier, while FAA requires background searches to be performed for all contractor employees, regardless of citizenship status, this policy is not being adequately enforced. FAA's failure to conduct background searches increases the risk that unauthorized individuals will gain access to FAA's facilities, information, or resources. In the case of code reviews, individuals intending harm may not bring to FAA's attention program errors that may have been detected during the code review process. In addition, copies of the code could be sold and/or reviewed to identify systems weaknesses that could later be exploited.

While the scope of our work did not include identifying instances of intrusions or illegal activities and we did not find any such instances during our review, FAA's failure to adhere to its own policies has increased the risk that its critical systems could be copied, distributed, and studied for weaknesses. Additionally, given the nature of code reviews, this type of activity may have occurred but not have been detected.

Conclusions

By not following sound security practices, FAA has increased the risk that inappropriate individuals may have gained access to its facilities, information, or resources. FAA has not adequately (1) enforced its policy requiring background searches of contractor employees,

---

[9]Because both contractors reviewed ARTS IIIA, there are a total of 21 code reviews on 20 systems.

(2) instructed its personnel on when to use the contract clause regarding citizenship requirements for contractor personnel, and (3) maintained records of all individuals assigned to work on mission-critical systems. FAA now faces a major task in assessing and addressing the increased risks to several of its mission-critical systems as a result of its failure to ensure that background searches were conducted. The implications of FAA's actions extend well beyond the Y2K date rollover and, as such, require FAA to act swiftly and decisively in its efforts to identify and mitigate the potential risk of intrusions and malicious attacks.

Recommendations

In order to address weaknesses in the enforcement of its policies and to identify and mitigate the risk of malicious intrusions or attacks on mission-critical FAA systems, we recommend that the FAA Administrator direct:

- FAA's Associate Administrator for Civil Aviation Security to clarify the requirements for contractor employee background investigations or checks and establish a process under which background investigations or checks are performed for all contractor staff where applicable. To increase the effectiveness of such an action, the Associate Administrator must also ensure that risk assessments are prepared with appropriate input from system owners and users.
- FAA's Associate Administrator for Research and Acquisitions to provide guidance on contract provisions, such as mandatory versus optional clauses, and enforce the appropriate use of these clauses. The Associate Administrator should instruct personnel to review current and pending contracts to ensure that all applicable contract provisions are included. In addition, the reasonableness of all clause limitations should be reviewed.
- The appropriate FAA entity to maintain records of the individuals, both FAA and contractor employees, working on systems, especially mission-critical applications.
- The appropriate FAA entity to perform security reviews of critical systems that have been remediated under contract.
- The appropriate FAA entity to carefully control access to and distribution of program source code, in conjunction with security reviews.
- The appropriate FAA entity to perform a risk assessment for code reviews conducted by Primeon to determine the potential exposure and consider retroactively performing background investigations of Primeon's staff.

Agency Comments

On December 13, 1999, we discussed the results of our review with FAA officials and incorporated their comments as appropriate. FAA officials agreed with our findings and the necessary corrective actions. Senior FAA officials also informed us that the agency had issued a policy memorandum effective December 10, 1999, calling attention to the requirements of FAA's personnel security program order. The agency has also begun the process of identifying the extent to which it or its contractors have performed background checks or investigations of contractor employees. In addition, FAA has tasked its Servicing

Security Elements organization with the responsibility of maintaining records of individuals, both FAA and contractor employees, who are working on systems.

On December 21 and 22, 1999, FAA officials, including the Acting Deputy Administrator, the Assistant Administrator for Information Services and Chief Information Officer, the Associate Administrator for Research and Acquisitions, and the Associate Administrator for Civil Aviation Security, provided additional comments. These officials stated that because FAA has five layers of systems protection, they believe that the risk of intrusion is extremely low. We anticipate evaluating FAA's layers of systems protection as part of our continuing efforts to monitor the agency's progress in addressing computer security weaknesses.

Objectives, Scope, and Methodology

As requested, our objectives were to determine whether FAA had policies governing the use of foreign nationals for Y2K code remediation activities, the extent to which foreign nationals and offshore facilities were used to remediate code, and the extent to which foreign nationals were involved in code reviews.

To achieve our objectives, we interviewed officials within several administrative offices,[10] the Y2K program office, and the Y2K program office for each respective line of business. We also contacted system representatives and officials of both the Facility Services and Engineering Division and Civil Aviation Security at the William J. Hughes Technical Center in Atlantic City, New Jersey.

To determine whether FAA had policies governing the use of foreign nationals for Y2K remediation activities, we met with officials and requested copies of policies developed by administrative offices within FAA. To assess the degree of foreign nationals and offshore facilities involvement in Y2K code remediation, we reviewed and analyzed information provided from the various Y2K program offices and interviewed system officials on a sample of mission-critical systems. To assess the degree of foreign national involvement in code review activities, we also reviewed and analyzed information provided by FAA officials. During the course of this review, we did not focus on identifying any instances of code tampering or other malicious activities.

We conducted our work at the Federal Aviation Administration in Washington, D.C., and the William J. Hughes Technical Center in Atlantic City, New Jersey. We performed our work from October through December 1999 in accordance with generally accepted government auditing standards.

We provided a copy of the briefing materials used in preparing this report to FAA and Department of Transportation (DOT) officials. FAA and DOT officials—including the Deputy Assistant Administrator of the Office of Information Services/Chief Information Officer (CIO), the Associate Administrator for Research and Acquisitions, the Chief of Staff

---

[10]These administrative offices included the Office of Information Services/Chief Information Officer, Office of Civil Aviation Security Operations, Office of Civil Aviation Security Policy and Planning, Office of Personnel, and Office of Acquisitions.

of the Office of the Administrator, the Director of Airway Facilities Service, the Year 2000 Program Office Manager, the Year 2000 Program Manager for Air Traffic Services, representatives from the Office of Civil Aviation Security and Office of Acquisitions, and a representative for the DOT CIO Office—provided oral comments on the briefing. In addition, we provided a draft of this letter to FAA for comment. We have incorporated FAA's comments as appropriate throughout this report.

- - - - -

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this report. At that time, we will send copies to Senator Robert F. Bennett, Senator Christopher J. Dodd, Senator Fred Thompson, Senator Joseph I. Lieberman, Senator Richard C. Shelby, Senator Frank R. Lautenberg, Senator Slade Gorton, Senator John D. Rockefeller IV, Representative Ralph M. Hall, Representative Constance A. Morella, Representative James A. Barcia, Representative Steven Horn, Representative Jim Turner, Representative Frank R. Wolf, Representative Martin O. Sabo, Representative John J. Duncan, and Representative William O. Lipinski in their capacities as Chair or Ranking Minority Members of Senate and House Committees and Subcommittees. We are also sending copies of this report to the Honorable Rodney E. Slater, Secretary of Transportation; the Honorable Jane Garvey, Administrator of the Federal Aviation Administration; the Honorable John Koskinen, Chairman of the President's Council on Year 2000 Conversion; and the Honorable Jacob J. Lew, Director of the Office of Management and Budget. Copies will also be made available to others upon request.

If you have any questions on matters discussed in this letter, please call me at (202) 512-6408 or Colleen Phillips, Assistant Director, at (202) 512-6326. We can also be reached by e-mail at willemssenj.aimd@gao.gov and phillipsc.aimd@gao.gov, respectively. Key contributors to this assignment were Cynthia Jackson, William Lew, and Keith Rhodes.
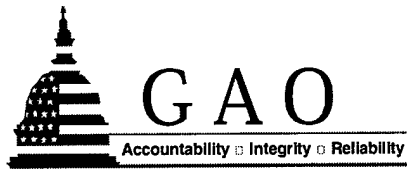
Sincerely yours,

[signed]

Joel C. Willemssen
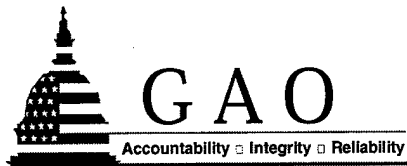Director, Civil Agencies Information Systems

G A O
Accountability □ Integrity □ Reliability

Use of Foreign Nationals in Year 2000
Code Remediation and Review Activities
at the Federal Aviation Administration

U.S. House of Representatives
Committee on Science
December 16, 1999

1

Briefing Overview

**G A O**
Accountability □ Integrity □ Reliability

- Objectives, Scope, and Methodology

- FAA Policies Governing Use of Foreign Nationals

- FAA's Utilization of Foreign Nationals or Offshore Entities to Remediate Code

- FAA's Utilization of Foreign Nationals to Review Code

- Summary of Observations

- Suggested Actions

2

GAO
Accountability □ Integrity □ Reliability
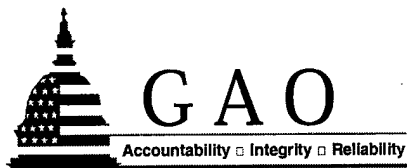
Objectives, Scope, and Methodology

Objectives

- Determine whether FAA has policies governing the use of foreign nationals for Year 2000 code remediation activities

- Determine the extent to which FAA used foreign nationals or offshore facilities to remediate code

- Determine the extent to which FAA used foreign nationals to perform code reviews
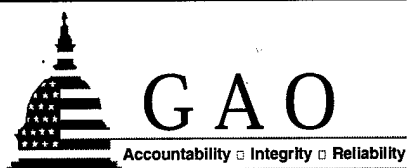
3

GAO
Accountability □ Integrity □ Reliability
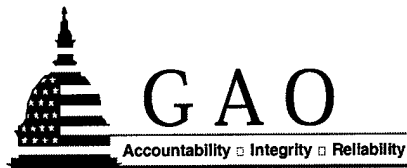
## Objectives, Scope, and Methodology (cont'd)

Scope

FAA

- Administrative Offices
- Year 2000 Program Office
- Year 2000 Program Office for each respective line of business (LOB)
- William J. Hughes Technical Center

4

Objectives, Scope, and Methodology (cont'd)

G A O
Accountability □ Integrity □ Reliability

Methodology

- Identified FAA policies governing the hiring of foreign nationals by FAA and contractors
- Assessed information on the use of foreign nationals and offshore entities to perform or oversee Year 2000 code remediation activities
- Interviewed FAA system officials on a sample of mission-critical systems
- Obtained FAA comments on a draft of the slides and incorporated changes as appropriate
- Performed work in accordance with generally accepted government auditing standards from October through December 1999
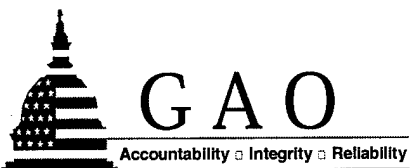
5

FAA Policies Governing Use of Foreign Nationals

GAO
Accountability ▫ Integrity ▫ Reliability

FAA's Personnel Security Program Order

- requires background investigations to be performed for FAA employees
- requires background checks or investigations to be performed for contractor employees who have comparable exposure to FAA's facilities, information, or resources, except for temporary contractor employees in low-risk positions
  - the type of background check or investigation required is based on the level of risk determined by the FAA system owner and users

However,

- the Year 2000 Program Office was unaware of this requirement
- we identified instances where background checks or investigations were not performed for contractor employees

6

G A O
Accountability □ Integrity □ Reliability
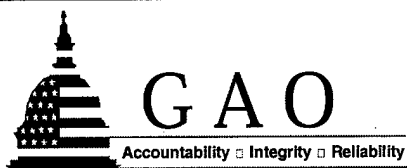
FAA Policies Governing Use of Foreign Nationals (cont'd)

FAA's Human Resource Policy Manual

- restricts hiring to U.S. citizens and nationals (residents of American Samoa and Guam) but allows for exceptions
  - FAA may hire foreign nationals if
    - there are an insufficient number of well-qualified applicants, and/or
    - there is an emergency, in which case, these individuals can be hired for a brief period of time

7

FAA Policies Governing Use of Foreign Nationals (cont'd)

GAO
Accountability □ Integrity □ Reliability
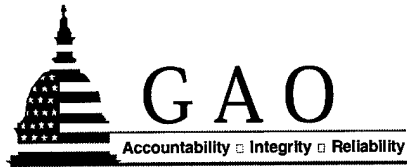
FAA's Required Contract Clause

* requires contractors to hire U.S. citizens or aliens who have been lawfully admitted for permanent residence as evidenced by a green card, or who meet other Immigration and Naturalization Service requirements

However, the clause

* is applicable only if contractor employees are likely to perform work at FAA locations
* some FAA employees consider the clause mandatory while others consider it optional

8

FAA Policies Governing Use of Foreign Nationals (cont'd)

GAO
Accountability □ Integrity □ Reliability
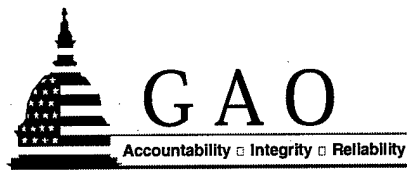
FAA's Required Contract Clause (cont'd)

* according to the Year 2000 Program Office, information was not readily available regarding the inclusion of this clause in current contracts

9

FAA's Utilization of Foreign Nationals for Y2K Code Remediation

G A O
Accountability □ Integrity □ Reliability
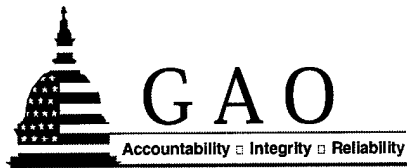
- Neither the Year 2000 Program Office nor the respective LOBs Year 2000 Program Offices routinely maintain information on the individuals who performed code remediation
  - FAA did not know if background checks or investigations were performed for contractor employees
    - Risk assessments were not prepared
  - However, according to FAA, remediation work was performed with existing contractors
- In response to our request for information on contract staff, FAA contacted the system owners and respective contracting firms and inquired as to the use of foreign nationals

10

FAA's Utilization of Foreign Nationals for Y2K Code Remediation (cont'd)

GAO
Accountability □ Integrity □ Reliability

Summary of foreign national involvement in FAA's Y2K code remediation activities

- 15 (10%) of 153 mission-critical (MC) systems had foreign nationals performing code repair and/or testing, according to FAA officials
  - 1 Commercial-off-the-shelf (COTS) system was remediated by a foreign-owned firm
    - ACT Telecommunications System was remediated by Northern Telecom, a Canadian firm
- The number of foreign nationals performing code repair and/or testing is not known for 4 (3%) of 153 MC systems

11

FAA's Utilization of Foreign Nationals for Y2K Code Remediation (cont'd)

GAO
Accountability □ Integrity □ Reliability

- Based on our review of information provided by FAA and our observations, we did not identify any FAA employees who were foreign nationals who performed code remediation
  - There were several instances where information was unavailable

- FAA does not know whether background checks or investigations were performed for all foreign national contractor employees who performed code remediation

12

FAA's Utilization of Foreign Nationals for Y2K Code Remediation (cont'd)

G A O
Accountability □ Integrity □ Reliability

Table 1: Summary of Reported Foreign National Involvement in Code Repair and/or Testing for Mission-Critical Systems Repaired

LOB	Number of MC systems requiring repair	Number of MC systems repaired with no foreign national involvement	Number of repaired MC systems with foreign national involvement	Number of MC systems repaired with foreign national involvement unknown
Associate Administrator for Research and Acquisitions (ARA)	26	15	7	4
Associate Administrator for Air Traffic Services (ATS)	65	63	2	0
Associate Administrator for Airports (ARP)	3	2	1	0
Administrative Systems (AAD)	50	49	1	0
Associate Administrator for Regulation and Certification (AVR)	6	2	4	0
Associate Administrator for Commercial Space Transportation (AST)	0	0	0	0
Associate Administrator for Civil Aviation Security (ACS)	3	3	0	0
Office of System Safety (ASY)	0	0	0	0
Totals	153	134	15	4

SOURCE: FAA

13

FAA's Utilization of Foreign Nationals for Y2K Code Remediation (cont'd)

GAO
Accountability ▫ Integrity ▫ Reliability

Table 2: Summary of Mission-Critical Systems Repaired with Reported Foreign National Involvement in Code Repair and/or Testing

LOB	System Name	Contractor Name	Number and nationality of foreign nationals	Contractor was foreign owned or controlled?	Code remediated offshore?	Comments
ARA	CTX 5000 (Explosive Detection System)	InVision	*	*	*	Commercial-off-the-shelf (COTS) product. Testing done utilizing German engineers
	ACT Telecommunications System[1]	Northern Telecom	*	Yes, Canadian	*	COTS product
	Traffic Flow Management Infrastructure-Enhanced Traffic Management System	Volpe	2 Chinese 1 Ethiopian 1 Irish 1 Ukrainian	No	Unknown	Contract staff involved in modification and testing activities
	Enterprise Network/Headquarters Data Network	AMTI	1 Venezuelan	No	No	COTS product
	Voice Switching and Control System[1]	Intellisource	*	*	*	FAA system representatives noted that there was 1 foreign national involved in testing at the Technical Center
	Oceanic Automation System	Raytheon	2 British	No	No	(
	Oceanic System Development and Support Products	Raytheon	2 British	No	No	

SOURCE: FAA
*--Information unavailable
[1]Information of the nationality of FAA employees also unavailable

14

FAA's Utilization of Foreign Nationals for Y2K Code Remediation (cont'd)

GAO
Accountability □ Integrity □ Reliability

Table 2: Summary of Mission-Critical Systems Repaired with Reported Foreign National Involvement in Code Repair and/or Testing (cont'd)

LOB	System Name	Contractor Name	Number and nationality of foreign nationals	Contractor was foreign owned or controlled?	Code remediated offshore?	Comments
ATS	Information Display System	Systems Atlanta, Inc.	1 Liberian	No	No	COTS product. Individual installed commercial off the shelf hardware
	National Airspace Data Interchange Network II	Hughes Network Systems, Dimensions International, TRIOS, DITCO, Technical Management Assistance	2 British	No	No	COTS product. Individuals were involved in testing
ARP	Air Carrier Activity Information System	Volpe	1 Japanese	No	No	Individual involved in program testing
AAD	Departmental Accounting and Financial Information System	MTSI	6 Malaysians, 1 Pakistanian, 1 India Citizen**	No	No	
		CEXEC	1 Vietnamese	No	No	

SOURCE: FAA
*--Information unavailable
**--However, the individual is now a United States citizen according to FAA

15

FAA's Utilization of Foreign Nationals for Y2K Code Remediation (cont'd)

G A O — Accountability □ Integrity □ Reliability

Table 2: Summary of Mission-Critical Systems Repaired with Reported Foreign National Involvement in Code Repair and/or Testing (cont'd)

LOB	System Name	Contractor Name	Number and nationality of foreign nationals	Contractor was foreign owned or controlled?	Code remediated offshore?	Comments
AVR	Online Aviation Safety Inspection System	Galaxy Scientific Corporation	5 **	No	No	
	Safety Performance Analysis System	Computer Sciences Corporation	1 India Citizen	No	No	
		Akuna Technologies, Inc.	1 Nigerian			
	Client Server Applications:					
	Financial Tracking System	JW Internet Technologies	1 Chinese 1 India Citizen	No	No	
	Air Transportation Oversight System	CGH, Inc	2 South Africans	No	No	
	Document Imaging Workflow Subsystem	Affiliated Computer Services	8 India Citizens	No	No	
	Electrocardiogram Subsystem	Mortara	1 Italian	No	No	
	Mainframe Application:					
	Integrated Safety Information System	OAO Corporation	1, nationality unknown	No	No	

SOURCE: FAA
*--Information unavailable
**--Contractor expressed privacy and discrimination concerns about releasing employees' countries of origin

16

FAA's Utilization of Foreign Nationals for Y2K Code Remediation (cont'd)

G A O
Accountability □ Integrity □ Reliability

Table 3: Summary of Mission-Critical Systems Repaired for which Foreign National Involvement in Code Repair and/or Testing is Unknown

LOB	System Name	Contractor Name	Number and nationality of foreign nationals	Contractor was foreign owned or controlled?	Code remediated offshore?	Comments
ARA	BandWidth Manager Network[1]	*	*	*	*	COTS product received from the Department of Defense
	Operation Support Telephone System[1]	*	*	*	*	COTS product
	ASU-400 Local Area Network	*	*	*	*	COTS product
	CCMail	Lotus Development Corporation	*	No	*	COTS product

SOURCE: FAA
*--Information unavailable
[1]Information on the nationality of FAA employees is also unavailable   17

FAA's Utilization of Foreign Nationals to Review Code

GAO
Accountability □ Integrity □ Reliability

FAA hired two contractors (Primeon and Computer Generated Solutions, Inc.) through the General Services Administration (GSA) to perform code reviews of 20 mission-critical systems

- Code reviews have been and continue to be performed to identify potential Year 2000 issues within the remediated code
    - The reviews entail a line-by-line analysis of a copy of the program source code to identify and evaluate date-related fields
    - For each system, a final report with the review results is provided to the appropriate Year 2000 Program Office and identified issues are expected to be addressed by system owners

18

FAA's Utilization of Foreign Nationals to Review Code (cont'd)

G A O
Accountability □ Integrity □ Reliability
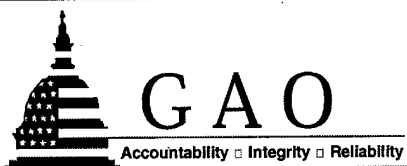
Year 2000 system code reviews

Primeon--
- Display System Replacement
- Automated Radar Terminal System (ARTS) IIIA***
- Common ARTS
- National Airspace System Resource System (Operational Data Management System)
- Voice Switching and Control System
- Traffic Flow Management Infrastructure Enhanced Traffic Management System
- Dynamic Ocean Track System Plus
- Host Interface Device/National Airspace System/Local Area Network

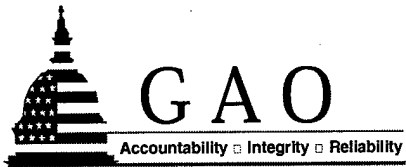**Computer Generated Solutions, Inc.--**
- ARTS IIIA***
- Flight Service Automation System
- U.S. Notices to Airmen System
- Terminal Doppler Weather Radar
- Aeronautical Information Systems-DEC Alpha
- HOST Environment*
- Micro-En Route Automated Radar Tracking System**
- Remote Maintenance Monitoring System*
- Integrated Communication Switching System Litton Type 2, 3
- Departmental Accounting and Financial Information System
- Integrated Personnel Payroll System
- Aviation Safety Analysis System
- Airport Air Carrier Reporting System

*--Code review in process
**--Code review tentatively scheduled
***--System reviewed by both Primeon and Computer Generated Solutions, Inc.
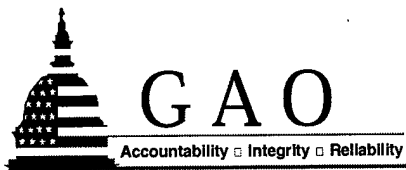
19

FAA's Utilization of Foreign Nationals to Review Code (cont'd)

GAO
Accountability □ Integrity □ Reliability

Primeon

- Neither the GSA contract nor FAA's statement of work under that contract prohibited the use of foreign nationals
  - contractor has a written internal security policy but does not perform background investigations of employees
    - employees are hired based on academic credentials and experience
- According to Primeon and FAA, 36 mainland Chinese nationals performed code reviews (4 with green cards, 32 with work visas)
- A nondisclosure agreement was signed by Primeon and certifications were provided to FAA denoting the return or pending destruction of the media and the purging of electronic copies of the code

20

FAA's Utilization of Foreign Nationals to Review Code (cont'd)

G A O
Accountability □ Integrity □ Reliability

Computer Generated Solutions, Inc. (CGS)

- Neither the GSA contract nor FAA's statement of work under that contract prohibited the use of foreign nationals
  - at FAA's request, contractor prepared a written internal security policy
  - contractor conducts a criminal background investigation prior to employment
- According to CGS and FAA, 1 Canadian national was involved in contract administration
- A nondisclosure agreement was signed by CGS requiring the return or destruction of all copies of software/firmware and all documentation provided by FAA or developed by CGS during its review

21

GAO
Accountability □ Integrity □ Reliability

Summary of Observations

- FAA has a policy that requires background checks or investigations to be performed for contractor employees based upon the level of risk associated with the project or task, however, the policy has not always been followed
- FAA has a contract clause that specifies the citizenship criteria for contractor employees, however,
  - the clause only applies if the contractor employees are likely to work at an FAA location
  - FAA employees have differing views as to whether the contract clause is mandatory or optional
- FAA did not maintain information on individuals assigned to perform code remediation and/or code reviews
- FAA does not know if background checks or investigations were performed for all foreign nationals involved in code remediation activities

22

GAO
Accountability □ Integrity □ Reliability

Summary of Observations (cont'd)

- One of FAA's two code review contractors did not conduct background investigations of its employees

By not following sound security practices, FAA introduces the risk of inappropriate individuals gaining access to FAA's facilities, information, or resources
- unauthorized changes, which are difficult to detect, could be made during code renovation
- program errors detected during testing and code reviews may not be identified for correction
- copies of the code could be sold and/or reviewed to identify system weaknesses that could later be exploited

23

GAO
Accountability □ Integrity □ Reliability

Suggested Actions

- Clarify requirements for contractor employee background checks or investigations, and establish a process to ensure that background checks or investigations are performed for all contractor staff where applicable
  - Ensure that risk assessments are prepared
- Provide guidance on contract provisions, such as mandatory versus optional clauses, and ensure that the clauses are used appropriately
  - Review current and pending contracts to ensure that all applicable contract provisions are included
  - Review reasonableness of clause limitations
- Maintain records of the individuals, both FAA and contractor employees, working on systems, especially mission-critical applications

24

GAO
Accountability □ Integrity □ Reliability

Suggested Actions (cont'd)

- Perform security reviews of critical systems that have been remediated

- In conjunction with security reviews, FAA should ensure that access to and distribution of programs is carefully controlled

- Perform a risk assessment for code reviews conducted by Primeon to determine the potential exposure and consider retroactively performing background investigations of Primeon's staff

(511818)

25